Password Authentication Protocol (PAP)

Subscriber authentication information (userid and password) is sent from the subscriber's computer to the ensoBox™ via Password Authentication Protocol. PAP is required to properly identify a subscriber prior to establishing a PPP connection to the ensoBox™.

PAP provides a simple method for a subscriber to establish its identity using a 2-way handshake. This is done only upon initial link establishment. After the link establishment phase is complete, a userid/password pair is repeatedly sent by the subscriber to the authenticator (in this case a RADIUS server) until authentication is acknowledged or the connection is terminated.

PAP is not a strong authentication method. Passwords are sent over the circuit "in the clear".

AAA (Authentication, Authorization, Accounting)

The ensoBox™ uses a RADIUS server to perform AAA functions (authentication, authorization, and accounting). The RADIUS server uses an LDAP (Lightweight Directory Access Protocol) server to retrieve subscriber authorization information (a list of services the user is allowed to access). Real-time accounting records are generated on the RADIUS server. Accounting records are sent from the ensoBox™ RADIUS server to the data center on a daily basis and used by the Billing Tool to generate subscriber bills.

Authentication – verifying that the subscriber is a valid subscriber by entering a valid userid/password.

Authorization – assigned services that can be accessed by an authenticated subscriber.

Accounting – collecting usage records for the length of the subscriber dial session.

Domain Name Service (DNS)

The ensoBox™ supports primary DNS for access to locally stored ensoServices™ and Secondary DNS for web browsing. Primary DNS for web browsing is supported at the ensoport.com™ data center. ensoBox™ components use the top level domain name of ensoport.com, and all components of the ensoBox™ will use the following naming convention:

<component>.<franchise city>.ensoport.com

where <component> identifies the node where the component is installed (Core, Access, or Services Node), and the component's functionality (router, switch, etc.).

Refer to the component naming conventions under the ensoBox^{TM} Components section of this document for more details about each component's DNS names.

Dynamic IP Addressing

The ensoBox^{TM} Remote Access Server (RAS) assigns dynamic IP addresses to subscribers each time a subscriber dials into an ensoBox^{TM}. The IP address assigned at the time the dial session is initiated is the same IP address that will be assigned to the subscriber for the entire session. The IP address will be terminated upon termination of the dial-up session and returned to the IP address pool and assigned to a future subscriber that initiates a dial session. Two (2) Class C Internet addresses are assigned for every 10,000 subscribers.

Network Based Data Storage

The ensoBox^{TM} uses a network attached storage (NAS) configuration to store end user data (email, web hosting information, files, etc.). Each subscriber is assigned a specific amount of storage space and will not be allowed to exceed that limit without authorization from his corresponding Franchise.

Data Backup

The ensoBox^{TM} performs scheduled backups of all applications and data. Backups will be stored on a tape jukebox, and tapes will be stored in a safe location, protected from fire, water, and any other harmful agents. Backups can be done hourly, daily, weekly, monthly, etc., and either full or partial.

Content Caching

The ensoBox^{TM} supports transparent content caching, where a local cache engine stores the most recently requested Internet data. If multiple subscribers request similar data, and the data's validity has not expired, then the data will be served from the local ensoBox^{TM} cache engine instead of from the original web server located somewhere within the Internet. This reduces Internet network delay and improves end user response time.

Content Filtering

The cache engine also allows the franchise to implement specific content filtering rules to prevent access to unwanted material on the Internet.

Security

ensoBox™ security is handled in a layered approach with attention given to host based security as well as network based security.

Host based security uses Wietse Venema's tcp-wrappers and manual hardening. TCP-wrappers are tools designed to provide greater control over all connections to the secured host. The manual hardening process will disable all unneeded services that could potentially be abused.

Network based security will be two fold, consisting of encryption of communications and access controls on the internal LANs within the ensoBox™. The encryption is accomplished using existing VPN features of the Cisco 2621 router. The router is configured to provide encryption of connections between the ensoport.com™ data center and the router within the ensoBox™. These connections are commonly referred to as VPNs. The other facet of network security involves securing access to the various networks within the ensoBox™. This is accomplished by designing the ensoBox™ such that equipment with similar access policies is located on similar Virtual LANs or VLANs. Access to VLANs is further protected by router based Access Control Lists (ACLs).

ensoServices™

The ensoBox™ offers the following services:

        ensoPortal™
        ensoMail™
        ensoWeb™
        ensoChat™
        ensoNews™
        anonymous FTP

ensoPortal™

The ensoPortal™ organizes subscriber data in such a way as to allow subscribers to more efficiently access ensoServices™ as well as other Internet-based services. The ensoPortal™ consists of